Amendments to the Claims

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for encryption comprising:

storing lock data which includes a group public key, an encrypted private key formed by encrypting a group private key ~~corresponding~~ that corresponds to said group public ~~key~~ key, by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of ~~the group/members~~ group members; and

encrypting encryption target data by use of the group public key of said lock data.

2. (Original) The method for encryption as claimed in claim 1, wherein said encryption target data is a decrypting key used for decrypting encrypted information.

3. (Currently Amended) A method for decrypting a cryptogram comprising:

storing lock data which includes a group public key, an encrypted private key formed by encrypting a group private key ~~corresponding~~ that corresponds to said group public ~~key~~ key, by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of ~~group/members~~ group members;

decrypting one of said encrypted common keys included in said lock data by use of a private key corresponding to ~~said group/member~~ a group member ~~used to generate said common key~~;

decrypting said encrypted private key included in said lock data by use of said decrypted common key used to generate said encrypted private key;

acquiring encryption target data encrypted by use of said group public key; and

decrypting said encrypted encryption target data by use of said decrypted group private key.

4. (Currently Amended) A method for writing a signature comprising:

storing lock data which includes a group public key, an encrypted private ~~key~~ key, the encrypted private key being formed by encrypting a group private key that corresponds ~~corresponding~~ to said public ~~key~~ key, by use of a common key, and a plurality of encrypted common keys generated by encrypting said common key by use of respective public keys of ~~the group/member~~ group members;

decrypting one of said encrypted common keys included in said lock data by use of ~~the~~ a private key corresponding to ~~said group/member~~ a group member ~~to generate said common key~~;

decrypting said encrypted private key included in said lock data by use of said decrypted common key ~~to generate said private key~~;

acquiring and storing signature target data on which a signature to be verified by use of said group public key is to be written; and

writing a signature on said signature target data by use of said decrypted group private key.

5. (Currently Amended) A method for generating lock data comprising:

acquiring a pair of a group public key and a group private key;

acquiring a common key;

encrypting said group private key by use of said common key to generate an encrypted private key;

encrypting said common key by use of public keys of respective ~~group/members~~ group members to generate corresponding encrypted common ~~key~~ keys; and

combining said public keys, said encrypted private key, and said encrypted common keys to generate lock data.

6. (Currently Amended) A method for generating lock data comprising:

acquiring a pair of a group public key and a group private key;

acquiring a common key;

modifying said group private key by use of a desired function including an inverse function to generate a modified group private key;

encrypting said modified group private key by use of said common key to generate an encrypted modified private key;

encrypting said common key by use of public keys of respective ~~group/members~~ group members to generate corresponding encrypted common keys; and

combining said public keys, said encrypted modified private key, and said encrypted common keys to generate lock data.

7. (Canceled)

8. (Original) The method for generating lock data as claimed in claim 5, wherein said lock data further includes a public key for verifying a signature, an encrypted signature private key which is formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, and a signature written by use of said signature private key on desired data included in said lock data.

9. (Currently Amended) A method for changing lock data comprising:

storing lock data including a first public key, an encrypted private key formed by encrypting a private key corresponding to said first public key by use of a common key, a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective ~~group/members~~ group members, a second public key for verifying a signature, an encrypted signature private key formed by encrypting a signature private key for

writing said signature by use of a public key of a changing right holder, said first public key, said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key;

decrypting said encrypted signature private key included in said lock data by use of said private key of a changing right holder;

changing said lock data; and

writing a signature on the changed lock data by use of said signature private key.

10. (Previously Presented) The method for changing lock data as claimed in claim 9, wherein said step for changing said lock data includes:

changing said second public key;

changing said signature private key;

changing said encrypted signature private key before changing by use of a new encrypted signature private key newly formed by encrypting a changed signature private key by use of said public key of a changing right holder; and

writing a signature by use of said signature private key after changing.

11. (Original) The method for changing lock data as claimed in claim 9, wherein said lock data has a version identifier that indicates the version of said lock data.

12. (Original) The method for changing lock data as claimed in claim 9, wherein said lock data has a precedent version dealing identifier, and controls how to deal with the lock data of the precedent version based on the identifier.

13. (Original) The method for changing lock data as claimed in claim 12, wherein said precedent version dealing identifier includes the information that identifies whether the change of said lock data should be applied retroactively or not.

14. (Currently Amended) A group lock including a public key, an encrypted private key formed by encrypting a group private key corresponding to said public key by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective ~~group/members~~ group members.

15. (Currently Amended) An apparatus for encryption comprising:

a memory part that stores a group public key, an encrypted private key formed by encrypting a group private key corresponding to said ~~common~~ group public ~~key~~ key, by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective ~~group/members~~ group members; and

an encryption part that encrypts encryption target data by use of a public key of said lock data.

16. (Currently Amended) An apparatus for decrypting ~~an cryptography~~ a cryptogram comprising:

a memory part that stores a group public key, an encrypted private key formed by encrypting a group private key corresponding to said ~~common~~ group public key by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective ~~group/members~~ group members;

a generation part that decrypts one of said encrypted common keys ~~included in said lock data~~ by use of ~~said~~ a private key corresponding to ~~said~~ a group member ~~group/member~~;

a generation part that decrypts said encrypted private key included in said lock data by use of said decrypted common key ~~to generate said private key~~;

an acquiring part that acquires encryption target data encrypted by use of said public key; and

a decrypting part that decrypts said encrypted encryption target data by ~~used~~ use of said decrypted group private key.

17. (Currently Amended) An apparatus for decrypting ~~an cryptography~~ a cryptogram comprising:

a memory part that stores a group public key, an encrypted private key formed by encrypting a group private key corresponding to said ~~common~~ group public ~~key~~ key, by use of a common key, and a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective ~~group/members~~ group members;

a generation part that decrypts one of said encrypted common keys ~~included in said lock data~~ by use of ~~said~~ a private key corresponding to a ~~group/member~~ group member;

a generation part that decrypts said encrypted private key included in said lock data by use of said decrypted common key ~~to generate said private key~~;

a memory part that stores and acquires signature target data on which a signature to be verified by use of said public key is to be written; and

a signature part that writes a signature on said signature target data by use of said decrypted group private key.

18. (Currently Amended) An apparatus for generating lock data comprising:

an acquiring part that acquires a pair of a group public key and a group private key;

an acquiring part that acquires a common key;

a generation part that encrypts said group private key by use of said common key to generate an encrypted private key;

a generation part that encrypts said common key by use of public keys of respective ~~group/members~~ group members to generate an encrypted common key; and

a generation part that combines said group public key, said encrypted private key, and said encrypted common key to generate lock data.

19. (Currently Amended) An apparatus for changing lock data comprising:

a memory part that stores lock data including a first public key, an encrypted private key formed by encrypting a private key corresponding to said first public key by use of a common key, a plurality of encrypted common keys formed by encrypting said common key by use of public keys of respective ~~group/members~~ group members, a second public key for verifying a signature, an encrypted signature private key formed by encrypting a signature private key for writing said signature by use of a public key of a changing right holder, said first public key, said encrypted private key, said encrypted common key, said second public key, and a signature written by use of said signature private key on said encrypted signature private key;

a generation part that decrypts said encrypted signature private key included in said lock data by use of said private key of a changing right holder to generate a signature private key;

a changing part that changes said lock data; and

a signature part that writes a signature on the changed lock data by use of said signature private key.